A Case Based Reasoning System for Automated Forensic Examinations

Graeme Horsman; Christopher Laing and Paul Vickers
School of Computing, Engineering and Information Sciences
Northumbria University
Newcastle-Upon-Tyne
graeme.horsman@unn.ac.uk

Abstract— **While still relatively young the use of digital forensics in criminal investigations is increasing. This has prompted law enforcement agencies to look at developing more efficient techniques for investigating digital media. Triage tools are seen as the next generation of digital forensics investigatory technologies. However, such tools are still lacking basic decision support mechanisms, and still require some form of human intervention. The authors propose to use a case based reasoning system to record and store digital forensics examinations. It is suggested that when coupled with knowledge based reasoning methods, a system would be a fully automated decision aide for digital forensic examinations. In outlining this proposal, this paper will review automation, triage, case-based reasoning, and then discuss the impact that knowledge reuse can have on digital investigations.**

Keywords: Forensics, Case based reasoning, Knowledge reuse, Triage

I. INTRODUCTION

The field of digital forensics (DF), while still relatively young [1] is driven by technological developments. Gogolin [2] points out that over 50% of reported criminal cases required the examination of a digital exhibit. On a global scale, cyber crime is on a dramatic rise [3] and shows no signs of decreasing [4]. This rising level of cybercrime is caused by the use of computerized technology to commit crimes meaning DF will become an increasing element in many criminal investigations [5]. The expanding use of technology to commit crime means High Tech Crime Units (HTCU) in the UK, now incur huge case backlogs, sometimes delaying investigations for up to a year[6] .

This paper discusses a novel approach to carrying out DF examinations; the use of knowledge sharing to create a fully automated investigatory process. It is suggested that Case-Based Reasoning (CBR) allows the capture and storage of DF investigator knowledge that can be reused in an attempt to identify the presence of evidence on a form of digital media. As noted by Sheldon [7] the reuse of previous case data, while learning from other examiners, also generates a central body of knowledge for sharing across the community. This would allow examinations to encapsulate expert knowledge from multiple sources, rather than becoming reliant on one principal investigator. Knowledge reuse would enable additional examiners to have their input into an investigation without having to be physically present [8]. This will create an automatic investigatory aide for examiners with the aim of reducing backlogs and improving DF case turnaround times.

II. WHAT IS AUTOMATION?

Backlogs and mounting issues with technological advancements are forcing HTCU to look at additional methods to efficiently analyse digital evidence. One such method is automation [9]. Automation can be viewed as a fast and transparent process performing repetitive activities that are currently undertaken by human experts [10]. However, Casey [9] believes that automation is only usefully when applied to routine tasks and because of the complexity of the data in any DF investigation, it cannot replace a trained examiner. Consequently, the separation between an automated process and human activities is the ability to make decisions and act upon them.

Current computer forensics tools are designed for evidence recovery rather than to assist in the investigation [5]. Ayers [11] points out that current forensics tools do not provide investigatory support to a sufficient level, and as such he describes them as ‘first generation’. In addition, these 'first generation' tools do not incorporate any type of decision support to aid the DF investigator [12]. While Garfinkel believes that too often tools are produced with the approach of obtaining ‘the lowest hanging fruit’ in mind [5].

Sheldon [7] believes that the idea of having one forensic expert for a case is no longer suitable. He feels that DF has moved on from when a single examiner’s understanding was adequate to complete an investigation and suggests that DF must unite to develop and reuse information [7].

III. REUSING DATA

Data reuse is an important element in the application of a CBR system used in DF investigations. For a CBR system to be able to deliver a reliable outcome, it has to learn or contain background knowledge of previous outcomes [13]. Reusing data from past cases to increase the knowledge of the CBR system, would allow it to determine whether cases fit within the bounds of previous offences. However, Scholtz, [8] undertook a survey of DF investigators and how they reused data from previous cases. It showed only 50% of participants feel they efficiently reuse data they have

ISBN: 978-1-902560-25-0

gathered from previous investigations. However, Kahvedzic [15] describes knowledge reuse as a way to systematically summarize the relevant information stored within a computer system to prove or disprove a criminal theory. Reusing data would therefore require the standardization of forensic examinations; allowing DF investigators to contribute their case work in a consistent and reusable way [8]. Unfortunately, at present there is no standard method or procedure for carrying out DF investigations, and it is this variety of approaches that leads to an incompatibility in the knowledge reuse from multiple examiners [16].

IV. EXISTING METHODS OF AUTOMATION

Triage is a process commonly used within medical care for sorting and prioritising patients for care [17]. Often triage is used at the scene of an accident or at an incident with where mass casualties are present. Triage was developed as a method to allocate what limited resources are available in the most effective way possible [17]. When adapted for the field of DF, triage can be thought of as a method of prioritising digital media for examination with the potential for removing redundant items [18]. In many cases triage in DF determines whether a submitted item will progress to a full examination, undertaken by an investigator. The prioritisation and preview of digital media is the main use for triage in the DF field [19]. Triage can occur both at the scene of a crime or within a forensic laboratory, but in both circumstances the aim is to provide a judgement on whether evidence exists whilst allocating as little time and resources as possible [18]. Mislan [20] provides a strong argument for an increase of triage usage, claiming the reduction in back logs and the increase in receiving intelligence from a device could potentially place less people at risk.

The DF field, although without accreditation, operates mainly under the supervision of ACPO [21]. Devised as guidelines, ACPO documentation is adhered to by most DF professionals and is seen as the most forensically sounds method for carrying out investigations. Forensic procedures mainly follow a strict flow of procedures known as device seizure, imaging, analysis and reporting. This, however, can change slightly when bringing in additional analysis methods such as triage as seen with Lim's forensic model [22]. Rogers has contributed 'The Cyber Forensic Field Triage Process Model' (CFFTPM) [14], a process of identifying and analysing data when limited time is available. This process consists of triaging key areas within a device including the home directory and common files such as internet history artefacts. This process is used to identify key exhibits for further examination but requires human review of data at all stages.

ADF's triage products [6] and Spektor forensics [24] [23] are both competitors in the triage market and claim to contain 'intelligent' information gathering techniques. One of which involves the capture of frequently accessed files and folders. This, however, only involves the analysis of timestamp activity and in many cases would return frequently accessed redundant files. Spektor claims to recover 'forensically useful' data and offers a facility to get assistance from additional examiners via a remote secure connection [23]. Although a novel technique, such a process goes against the principles of triage and in fact becomes a greater drain on resources by requiring the attention of two or more examiners.

Perry [25] highlights the importance of triage in the field of battle where soldiers are constantly locating digital storage media containing strong suspect links to terrorism. In such volatile situations it is imperative to analyse exhibits quickly to make a judgement of the relevance of any data it may contain. In situations like this it is impossible to undertake a full investigation therefore triage must operate at a high level of accuracy. When time is limited the reuse of previous data gathered from terrorism scenarios is not implemented. However, previous intelligence could have greater effect in profiling and identifying evidence quickly.

Triage tools do not always offer a satisfactory solution but automated information retrieval is a potential solution. In such a short space of time it is impossible to carry out a full examination therefore a process which retrieves relevant information can be more efficient. The current triage process in DF is limited in its capabilities and in many situations is restricted to certain crime types [6]. It can be argued that triage works best when a known set of files are to be identified whether by hash or file type and is mainly used in cases involving indecent images of children (IIC) [6]. Existing triage tools do not offer the adequate facilities for an on-scene investigation and attempt to fulfil the role of an in-lab forensic examination [20]. Most triage tools require the human review of information before a decision can be made, yet when large sets of information are returned it takes time for an examiner to make a decision on the relevance of each exhibit and any evidence it contains. Triage tools tend to be descendants from full forensic investigatory tools and perform parsing processes across relevant files and logs. This approach brings back the maximum amount for data for review, defeating the purpose of a quick analysis.

V. CASE BASED REASONING

Case based reasoning (CBR) is an approach to problem solving whereby known solutions from past problems are reused or adapted to solve current problems [26] [27] . A CBR system selects a case from its case knowledge base that gives the best solution for a given problem. New cases are frequently added to the knowledge base to increase CBR systems capacity for creating solutions [27] with each considered as a solution to a particular problem [28]. CBR systems have the ability to handle complex data for multifaceted problems [29] and prove useful in fields where there is a large body of unstructured data [30]. CBR systems are prominent in medical diagnosis, law and engineering environments where a known solution is present for solving tasks through previous knowledge reuse [31] [28] .

CBR systems offer the DF field an alternative approach to investigations. Treating each physical examination as a case in a CBR systems case base, all processes and relevant data

found by an investigator can be automatically reapplied to a new case. As many offences of the same crime type contain similar artefacts and evidence, a CBR system can determine how closely both cases match one another giving an indication of relevance of any data found on the target drive. This papers proposal of knowledge reuse for the automation of examinations can be facilitated through CBR systems, producing a novel approach to investigating digital media. With CBR, the DF field has the appropriate structures to facilitate knowledge reuse from previous investigations.

CBR systems rely on 4 functions in order to create a repeatable process. These states are:

- Retrieve. The retrieval stage requires the system to find the case that provides the best solution to the problem [32].
- Reuse. This involves reusing the case for problem solving [32].
- Revise. This adapts the proposed case if a better solution exists [32].
- Retain. Keeping the case for future use [32].

A CBR system selects a case from its knowledge base that fits best to creating a solution. New cases are all added to the knowledge base to increase its capacity for creating solutions [27]. Each case is considered a solution to a particular problem [28].
CBR systems are dependent on the cases they retain in their knowledge base to perform to the highest level [29]. Salomos [29] approach to CBR systems is one that fits well within the working principles of DF. He believes that redundant cases should be updated and removed as new techniques and procedures are released. This is similar to the way in which humans problem solve, when a better or more efficient method is deduced to solve a problem, the old redundant method is removed. A similar principle can be seen in DF, when improved procedures are developed, other methods are no longer used. The disadvantages of removing redundant cases is that should a problem require an old solution, the knowledge base is no longer capable of carrying out the task as it does not possess the knowledge.
CBR systems have the ability to handle complex data for multifaceted problems [29] and prove useful in fields where there is large bodies of unstructured data [30] seen with DF. CBR can bring a uniformed approach to DF investigations and give all members of the field the ability to contribute their knowledge from the cases they investigate.

VI. KNOWLEDGE BASES

The role of the knowledge base (KB) is to house facts or knowledge regarding the domain in which it operates [33]. Many systems that employ KBs are expected to create hypothesises as well as simply stating facts therefore a KB must also maintain a rule set that determines its operation [33]. KBs often house large sets of data and must be designed to cope with a potentially ever expanding set of knowledge [34]. Their structure allows for the domain knowledge from DF to be housed for reuse later in the CBR systems operation. In the case of CBR systems the KB contains individual cases, also known as a case base.

KBs are in a machine readable format that allows knowledge to be automatically queried and maintained [35]. A KB is the foundation from which a CBR system operates. The KB is often populated by a knowledge engineer who is an expert in the domain that the CBR system is operating in [36]. It is at this stage in the design that knowledge needs to take a form that can be processed and reused later.

One of the main issues faced during the creation of a KB for this thesis is that most KBs store fragments of facts regarding a topic and not a complete solution. When using a KB for DF investigations, a greater detail of knowledge would be stored. For example, it is not acceptable for a KB to only identify Internet browsing history on a suspect machine. Such history must be analysed and classified to see if it is relevant. There is also very little chance when carrying out DF investigations that a direct match will occur. Many KBs record information in a format which can be queried with true or false values. In many DF investigations, relevant data varies in detail, therefore a fuzzy match most occur. KBs are often incomplete as a complete solution too many problems involves an infinite amount of data which is simply not possible to implement [37]. Knowledge is only added to KBs if and when it is available. This is why many knowledge bases must be able to solve problems with the knowledge they contain. To create KBs, a precise knowledge of the domain must be gathered which can impact on the length of time it takes for KB creation [27].

Every piece of knowledge in a KB has significance to problem solving and forms links to other stored data which forms the reliability of a given output. The KB relies on these links to enforce the decisions it makes, treating each one as a fact. Should these links become contradictory with the introduction of new knowledge or incorrect knowledge, the KB is compromised [38]. Santos [38] suggests that KBs currently lack the flexibility to acquire new data and additional methods such as Bayesian networks should be explored.

VII. KNOWLEDGE GATHERING

Expert Engineers (EE) are considered to be experts in their domain. The population of a KB is commonly completed by an EE as the reliability of the system depends on the quality of its knowledge. An EE is expected to verify data as it passes into the KB to ensure that it is both correct and suitable for the given purpose [33]. The EE is also expected to determine patterns and links between knowledge to ensure that the KB returns accurate answers to any queries it may face [33].

For the scope of this paper, an EE can be any DF examiner working within the field. Should such a system be incorporated in DF, contributions from many investigators would be required and therefore responsible for acting as an EE. This causes problems in the vetting of a person's ability

to examine digital media and the quality of work they produce. A system implemented on such a large scale would in most probability incur a large quantity of human error during the KB population stage. To ensure the reliability of the system, it would require an additional and more senior EE to valid all inputs [37]. All KBs must be tested to ensure that both the KB and an expert give the same answer when asked the same question [40]. This ensures the intelligence of a system and gives a measure of accuracy and reliance. Errors found in KBs can affect the way in which it functions and in many circumstances, actions are not taken to rectify errors due the complexity of the given task [40].

The complexity of building a KB and with EE deciding the relevance of data subjectively, the KBs validity cannot always be guaranteed on completion [37]. It is important that the EE enforces strict rules during new knowledge acquisition to ensure the KB is semantically sound. This ensures that all data both new and old is stored in a format that can still carry out problem solving within its target domain [38]. A EEs goal is to 'have an approach that guarantees precise and intuitive local semantics while minimizing the maintenance expense of global semantic consistency' [38]. A KB's ability to problem solve should not be jeopardised by the introduction of new data.

This knowledge must be gathered over a finite period of time across multiple sources to ensure there is enough depth [41]. For such data to be recognisably accurate, it must be validated as acceptable and correct at some point prior to the evidence collection by a DF investigator. Therefore the development of such a practice must incur a period of learning before it is suitable for use. Problems are also present when the background gathered knowledge does not contain the relevant information for a suspected offence [41].

VIII. CONCEPT OF PROFILING

Profiling crimes is a technique used since the 15th century [3] to identify characteristics of an offender or offence, usually unknown and identified through previously gathered data from committed offences or offenders [39]. Ruibin [43] believes that adapting current forensic methods and practices to incorporate profiling as a means to automate forensics is a way to combat the demands placed on DF investigators. Profiling each investigation can produce a set of unique features regarding the specific crime. These features when used to produce a profile can then be used to cross examine further drives for similarities in both investigations.

Baumgartner's believed that profiling could generate links and patterns between current and past data showing instantly if dangerous correlations exist in behaviour of suspected offenders [39]. This system contains methods for carrying out profiling from a police database containing relevant knowledge for the system to learn from. Baumgartner's profiling system was shown to be more accurate in tests than three profiling experts when correctly identifying a suspect's guilt. Replicating this success when applying profiling principles to the proposed CBR system for DF investigations can change the way the field operates.

Rogers [4] highlights both the need and want for offender profiles to be generated from digital evidence to improve the way examiners approach investigations. At present a lack of data from very few investigators taking this approach is what has stopped profiling in DF from making an impact in the way an examination is carried out [4]. Arthur's Forensic Evidence Management System (FEMS) [1] is one of the few attempts made to provide a method to profile evidence on a target drive for reuse in later automated examinations. Their system allows the examiner to predict what evidence might exist on a machine and query the profiling software to see if the storage medium fits within the bounds of known suspect features and knowledge it already contains [1]. The key component of the FEMS system is the ability to update and relearn data on a case by case basis.

Corney's [42] approach to profiling systems focuses on the analysis of user profiles storage on a Windows XP system. A learning process is required for an automated profiling system to work, however he approaches it from a live analysis perspective. In order to profile, a user's activity must be monitored whilst carried out in real time, unlike the FEMS model [1]. Corney's goal is to recognise anomalous events and event patterns [42]; however, anomalous events are not confined to within the user's profile on a system. He also relied heavily on the tracking of processes that were executed within the confines of the system. A weakness of this is that not all malicious activity is carried out using malicious software. It is common for applications such as Internet Explorer to carry out both innocent and harmful tasks. Similar approaches to profiling can be seen with Kahai's [45] system where live events are profiled as they occur. Both Kahai and Corney's systems carry out similar tasks to intrusion detection systems.

For the technique of profiling to be successful it is dependent on the accuracy and value of the data it has gathered and stored from previous cases [46]. Therefore a great reliance is place upon the way in which a profiling system collects its knowledge. The initial stages of an investigation often present a DF examiner with the hardest part of an investigation as it contains the greatest amount of data to examine [44]. At this stage in an investigation, profiling can be used as a quick and efficient way to highlight potential evidence seen from previous cases and determine the direction an investigation takes. Profiles of already known offences can help the investigator to direct their searches and determine the relevance of data stored on the drive [44].

When a DF investigation commences, the initial searching of a device is the point in which both redundant and evidential data is identified [47]. It is often challenging at this point to determine the relevance that any evidence has to a committed offence [12].

IX. CONCLUSION

This article presents the proposal of an automated CBR system for the creation of an automated examination aide for forensic investigators. CBR systems have already proved a success in other disciplines, encapsulation expert knowledge for automatic decision support. When applied to DF, CBR systems have the potential to be a success, taking advantage of their ability to process complex problems without human interaction. This approach will allow investigators to query evidence and produce a preliminary verdict on its content, without the need for human interaction or review of data. CBR systems offer workable structures to store and query domain knowledge. For DF to progress as a field and take advantage of knowledge reuse, a CBRs case base offers a unique way to record past investigations and take advantages of investigations that have already been carried out

.

Issues such as a standardisation strategy for the way in which data is collected have yet to be solved. However, the collective knowledge of multiple examiners when stored in a CBR system and combined with strategic reasoning methods, can offer an approach to investigations where the KB is smarter than any one given examiner. This approach also allows the field to collate knowledge for the collective use, moving towards the goal of successfully examining digital evidence.

REFERENCES

[1] Arthur, K. K.; Olivier, M. S.; Venter, H. S. & Eloff, J. H.
Considerations Towards a Cyber Crime Profiling System
The Third International Conference on Availability, Reliability and Security, **2008**

[2] Gogolin, G. The Digital Crime Tsunami
Digital Investigation, **2010**, *7*, 3-8

[3] Nykodym, N.; Taylor, R. & Vilela, J.
Criminal profiling and insider cyber crime
Digital Investigation, **2005**, *2*, 261-267

[4] Rogers, M. K.; Seigfried, K. & Tidkea, K.
Self-reported computer criminal behavior: A psychological analysis
Digital Investigation, **2006**, *3*, 116-120

[5] Garfinkel, S. L.
Digital forensics research: The next 10 years
Digital Investigation, **2010**, *7*, 64-73

[6] ADF
Triage Solutions for Evidence and Intelligence Aquisition
2010 Accessed: 24th March 2011

[7] Sheldon, A.
The future of forensic computing
Digital Investigation, **2005**, *2*, 31-35

[8] Scholtz, J. & Narayanan, A.
Towards an Automated Digital Data Forensic Model with specific reference to Investigation Processes
Proceedings of the 8th Australian Digital Forensics Conference, **2010**

[9] Casey, E. & Friedberg, S.
Moving forward in a changing landscape
Digital Investigation, **2006**, *3*, 1-2

[10] Nogueira, J. H. M. & Júnior, J. C.
Autonomic Forensics a New Frontier to Computer Crime Investigation Management
The International Journal of Forensic Computer Science, **2009**, *1*, 29-41

[11] Ayers, D.
A second generation computer forensic analysis system
Digital Investigation, **2009**, *34-42*, 6

[12] Hoelz, B. W. P.; Ralha, C. G.; Geeverghese, R. & Junior, H. C.
Cooperative Multi-agent Approach to Computer Forensics
Web Intelligence and Intelligent Agent Technology, 2008. WI-IAT '08. IEEE/WIC/ACM International Conference, **2008**

[13] Mehrotra, K.; Mohan, C. K. & Ranka, S. *(Eds.)*
Elements of artificial neural networks
MIT Press, **1997**

[14] Rogers, M. K.; , Goldman, J.; Mislan, R.; Wedge, T. & Debrota, S.
Computer Forensics Field Triage Process Model
Journal of Digital Forensics, Security and Law, **2006**, *1*, 19-38

[15] Kahvedzic, D. & Kechadi, T.
DIALOG: A framework for modeling, analysis and reuse of digital forensic knowledge
Digital Investigation, **2009**, *6*, 23-33

[16] Hoss, A. M. & Carver, D. L.
Weaving ontologies to support digital forensic analysis
Intelligence and Security Informatics, 2009. ISI '09. IEEE International Conference, **2009**

[17] Weinerman, R. E.; Rutzen, R. S. & Pearson, D. A.
Effects of Medical Triage in Hospital Emergency Service
Yale Studies in Ambulatory Medical Care, **1965**, *80*, 389-399

[18] Parsonage, H.
Computer Forensics Case Assessment and Triage
2009

[19] Hunton, P.
The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation
Computer Law & Security Review, **2011**, *27*, 61-67

[20] Mislan, R. P.; Casey, E. & Kessler, G. C.
The growing need for on-scene triage of mobile devices
Digital Investigation, **2010**, *6*, 112-124

[21] Association of Chief Police Officers
Good Practice Guide for Computer-Based Electronic Evidence
2007

[22] Lim, K.-S.; Lee, S. & Lee, S.
Applying a Stepwise Forensic Approach to Incident Response and Computer Usage Analysis
Computer Science and its Applications, 2009. CSA '09. 2nd International Conference, **2009**

[23] Gold, S.
The black art of digital forensics
Infosecurity, **2009**, *6*, 12-15

[24] Talks, E.
SPEKTOR® Forensic Intelligence-Forensic Triage
Accessed: 24th March 2011

[25] Perry, W. G.
Information Warfare: Assuring Digital Intelligence Collection
2009

[26] Lee, M.
A study of an automatic learning model of adaptation knowledge for case base reasoning
Information Sciences, **2003**, *155*, 61-78

[27] Kumar, S. & Raj, D.
A Contemporary Approach to Hybrid Expert Systems
International Conference on Computer and Communication Technology (ICCCT), **2010**

[28] Aamodt, A. & Plaza, E.
Case-Based Reasoning: Foundational Issues, Methodological Variations, and System Approaches
AI Communications, **1994**, *7*, 39-59

[29] Salamo, M. & Lopez-Sanchez, M.
Adaptive case-based reasoning using retention and forgetting strategies
Knowledge-Based Systems, **2011**, *24*, 230-247

[30] Madhusudan, T.; Zhao, J. L. & Marshall, B.
A case-based reasoning framework for workflow model management
Data & Knowledge Engineering, **2004**, *50*, 87-115

[31] Craw, S.
Case Based Reasoning
2005

Accessed: 24th March 2011

[32] Lopes, E. C.
A Decision Support Methodology for the Control of Alternative Penalties - A Case-Based Reasoning Approach
International Conference on Information, Process, and Knowledge Management, **2009**

[33] Velasquez, J. D. & Palade, V.
A Knowledge Base for the maintenance of knowledge extracted from web data
Knowledge-Based Systems, **2007**, *20*, 238-248

[34] Kingston, J.
High Performance Knowledge Bases: four approaches to knowledge acquisition, representation and reasoning for workaround planning
Expert Systems with Applications, **2001**, *21*, 181-190

[35] Alani, H.; Kim, S.; Millard, D.; Weal, M.; Hall, W.; Lewis, P. & Shadbolt, N.
Automatic ontology-based knowledge extraction from Web documents
Intelligent Systems, IEEE, **2003**

[36] Mohamad, N. R.; Daut, N. & Jaaman, S. A.
Development of expert system for identifying dolphins species in Malaysian fisheries using PROLOG
Information Technology, **2008**

[37] Santos, J. E. & Dinh, H. T.
On automatic knowledge validation for Bayesian knowledge bases
Data and Knowledge Engineering, **2008**, *64*, 218-241

[38] Santos, J. E.; Santos, E. S. & Shimony, S. E.
Implicitly preserving semantics during incremental knowledge base acquisition under uncertainty
International Journal of Approximate Reasoning, **2003**, *33*, 71-94

[39] Baumgartner, K.; Ferrari, S. & Palermo, G.
Constructing Bayesian networks for criminal profiling from limited data
Knowledge-Based Systems, **2008**, *21*, 563–572

[40] Gonzalez, A. J. & Barr, V.
Validation and verification of intelligent systems – what are they and how are they different?
Journal of Experimental and Theoretical Artificial Intelligence, **2000**, *12*, 407-420

[41] Liu, Z.; Lin, D. & Guo, F.
A Method for Locating Digital Evidences with Outlier Detection Using Support Vector Machine
International Journal of Network Security, **2008**, *6*, 301-308

[42] Corney, M.; Mohay, G. & Clark, A.
Detection of Anomalies from User Profiles Generated from System Logs
9th Australasian Information Security Conference (AISC 2011),, **2011**

[43] Ruibin, G. & Gaertner, M.
Case-relevance information investigation: binding computer intelligence to the current computer forensic framework
International Journal of Digital Evidence, **2005**, *4*, 1-13

[44] Rogers, M.
The role of criminal profiling in the computer forensics process
2003

Accessed: 24th March 2011

[45] Kahai, P.; Srinivasan, M.; Namuduri, K. R. & Pendse, R.
Forensic Profiling System
2005

[46] Schermer, B. W.
The limits of privacy in automated profiling and data mining
Digital Law and Security Review, **2011**, *27*, 4 5 e5 2

[47] Carrier, B. D. & Spafford, E. H.
Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence
DFRWS, **2005**